

# FortiClient Enterprise Management Server - QuickStart Guide

VERSION 1.0.1

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



June 24, 2016

FortiClient Enterprise Management Server 1.0.1 QuickStart Guide

04-101-253016-20160624

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
Supported installation platforms	5
Deployment options	6
Standalone	6
Integrated FortiGate	6
<b>Install</b>	<b>8</b>
Download the installer	8
Install FortiClient EMS	8
Start FortiClient EMS	9
Access FortiClient EMS remotely	10
Configure user accounts	10
<b>Set Up Endpoint Management</b>	<b>11</b>
Discover endpoints	11
Use AD servers to discover endpoints	12
Scan local workgroups to discover endpoints	12
FortiClient Telemetry Gateway IP Lists	13
Create FortiClient Telemetry Gateway IP Lists	13
Assign FortiClient Telemetry Gateway IP Lists	13
FortiClient installers	13
Endpoint profiles	15
Create endpoint profiles	15
Import FortiClient profiles from FortiGate	17
Connect FortiClient Telemetry to FortiClient EMS	18

## Change Log

Date	Change Description
2015-10-13	Initial release of 1.0
2016-06-24	Updated for 1.0.1

# Introduction

This guide describes how to install and set up FortiClient Enterprise Management Server (EMS) for the first time.

FortiClient EMS is used to deploy and manage FortiClient endpoints.

## Supported installation platforms

You can install EMS on the following platforms:

- Microsoft Windows Server 2012, 2012 R2
- Microsoft Windows Server 2008 R2



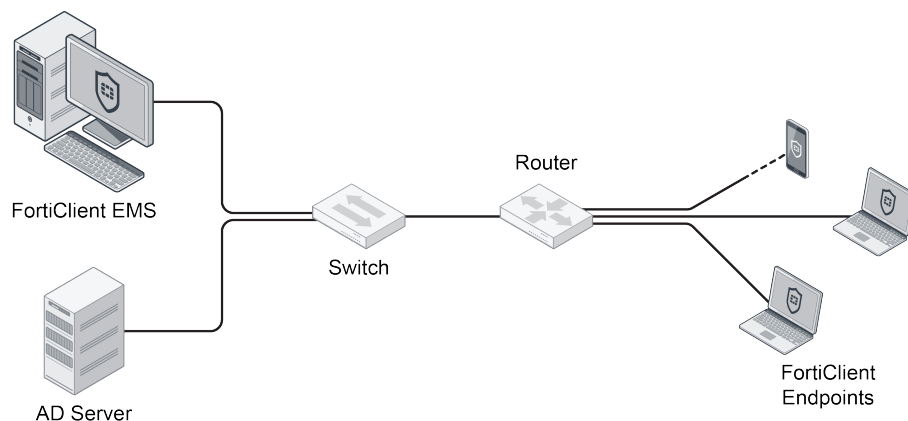
For information about minimum system requirements and the latest information about supported platforms, see the *FortiClient EMS Release Notes*, available in the [Fortinet Document Library](#).

---

## Deployment options

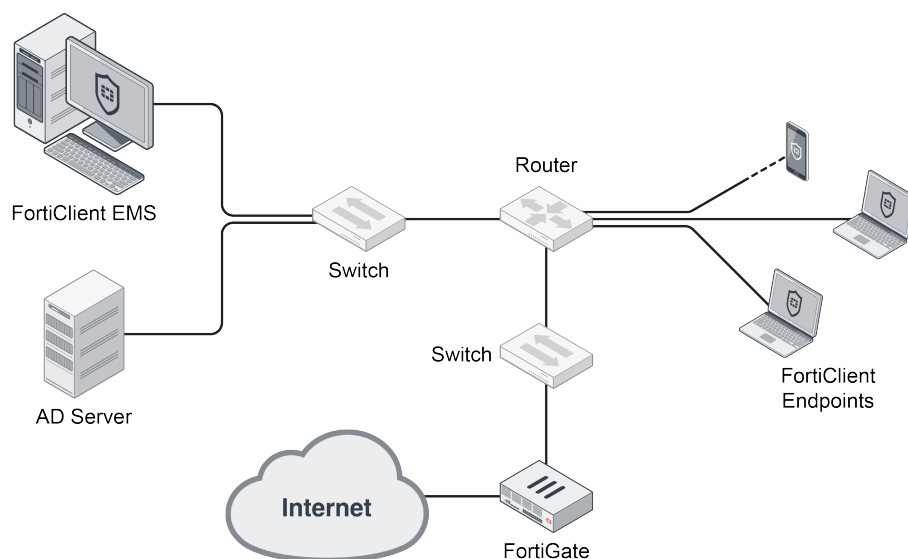
The following deployment options for EMS are supported: standalone or Integrated FortiGate.

### Standalone



In standalone mode, a FortiGate device is not required, and network access compliance (NAC) is not supported. In a standalone mode, EMS deploys FortiClient software on endpoints, and FortiClient endpoints connect FortiClient Telemetry to EMS to receive configuration information from EMS. EMS is used to deploy, configure, and monitor FortiClient endpoints.

### Integrated FortiGate



In integrated mode, a FortiGate device is required, and NAC is supported. In integrated mode, EMS deploys FortiClient software on endpoints, and FortiClient endpoints connect FortiClient Telemetry to FortiGate. FortiClient endpoints also connect to EMS for real-time monitoring. After FortiClient endpoints are connected, a

FortiClient profile with compliance rules is downloaded from FortiGate to the endpoint. Depending on the settings in the FortiClient profile from FortiGate, a profile of FortiClient configuration information might also be downloaded from EMS to endpoints. FortiClient endpoints are now managed, and NAC is enforced.

FortiClient uses the compliance rules from FortiGate to communicate whether the endpoint is compliant. If an endpoint fails to meet the compliance rules, the steps required to remain compliant are communicated. For more information, see the *FortiClient Administration Guide*.

# Install

For full network protection, FortiClient EMS should be installed on a server with FortiClient installed on all of your endpoint devices.



EMS listens on TCP port 8013 for FortiClient connections.  
TCP ports 443 and 10443 are also required for EMS operation.

---

After completing the installation of FortiClient EMS, the following services should be running:

- FortiClient Enterprise Management Server Apache Service
- FortiClient Enterprise Management Server Active Directory Service
- FortiClient Enterprise Management Server Service
- FortiClient Enterprise Management Server Update Service.

For information about upgrading FortiClient EMS 1.0 and later, see the *FortiClient EMS Release Notes*.

## Download the installer

FortiClient EMS is available for download from the following locations:

- FortiClient website: <http://forticlient.com/>
- Fortinet Support website: <https://support.fortinet.com/>

For more information about obtaining FortiClient EMS, contact your Fortinet reseller.

## Install FortiClient EMS

The FortiClient EMS installation package includes:

- FortiClient EMS
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server



Local administrator rights and Internet access are required to install FortiClient EMS.

---

### To install FortiClient EMS:

1. If you are logged into the system as an administrator, double-click the downloaded installation file.  
If you are not logged in as an administrator, right-click on the installation file, and select *Run as administrator* from the pop-up menu.
2. If applicable, select *Yes* in the *User Account Control* window to allow the program to make changes to your system.

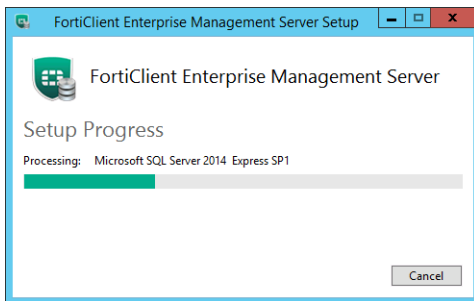


3. In the installation window, select *I agree to the license terms and conditions*, if you agree with the license terms and conditions. If you do not agree, you cannot install the software.

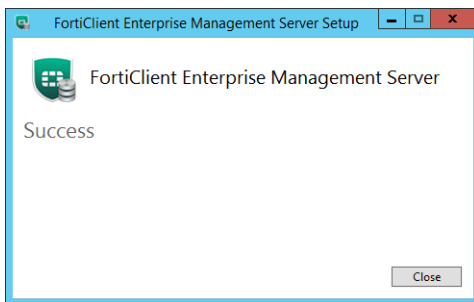


4. Select *Install*.

The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others. Please be patient.



5. When the program has installed correctly, the *Success* window will be displayed. Select *Close* to close the window.



A FortiClient EMS icon will be added to the desktop.

## Start FortiClient EMS

### To start FortiClient EMS:

1. Double-click the *FortiClient Enterprise Management Server* icon to start FortiClient EMS.
2. Sign in with username *admin* and no password.
3. Change the username and password by going to *View > User Management > Administration*.
4. Configure the endpoint server and client settings, including the IP address that FortiClient EMS will listen on, by going to *View > Settings*.

## Access FortiClient EMS remotely

You can access FortiClient EMS remotely by using a web browser instead of the GUI.

### To enable remote access to FortiClient EMS:

1. Go to *View > Settings*.
2. Enable *Remote Administration HTTPS Access*.
3. Select *Save*.

### To remotely access FortiClient EMS:

- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`

Ensure that you can ping `<server_name>` remotely. This can be achieved by adding it into a DNS entry or by adding it to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

## Configure user accounts

You can configure users to have no access to FortiClient EMS, or you can configure users to have administrator access to FortiClient EMS. You can configure local Windows users, LDAP users, or both local Windows users and LDAP users.

For local Windows users, the list of users is derived from the server on which FortiClient EMS is installed. If you want to add more users, you must add them to the server.

For LDAP users, you must add an LDAP server to FortiClient EMS, and then configure users.

### To add a LDAP server:

1. Go *View > User Management*.
2. Select the *LDAP Server* tab.
3. Configure the options, and click *Test*.
4. If the test is successful, select *Save*.

### To configure users:

1. Go to *View > User Management*.
2. Click the *+Add* from the toolbar.
3. In the *Add User* list, select *Windows User* or *LDAP User*.  
The *LDAP User* options is available only after you add an LDAP server to FortiClient EMS.
4. Select the specific domain access for the user.
5. Configure the permissions.
6. Click *Save*.

# Set Up Endpoint Management

This section describes how to set up FortiClient EMS for endpoint management.

Endpoints connecting FortiClient Telemetry to FortiClient EMS or FortiGate have profiles applied to them, and have virus scans run on them. FortiClient EMS can also force endpoints to install FortiClient, and then register to either EMS or FortiGate. See [FortiClient installers on page 13](#).

Endpoints imported from an AD server may already have a structured organization, or containers and computers discovered from the local network may already belong to a workgroup. If you want to change these pre-existing structures, you can create custom groups in EMS by right-clicking in the *Domains* or *Workgroups* section and selecting *Create Group*. You can move endpoints or other groups into the custom groups by right clicking on them and selecting *Move to*.

The EMS administrator can apply profiles to groups at any level. Nested groups with unassigned profiles inherit profiles from their immediate parent group.

## To set up endpoints:

1. Discover endpoints by adding domains and/or discovering local endpoints. See [Discover endpoints on page 11](#).
2. Create FortiClient Telemetry Gateway IP Lists and assign the lists to domains or workgroups. See [FortiClient Telemetry Gateway IP Lists on page 13](#).  
Alternately, you can add a FortiClient Telemetry Gateway IP List to a custom FortiClient installer by using the FortiClient Configurator tool.
3. Add a FortiClient installer to EMS. See [FortiClient installers on page 13](#).
4. Create an endpoint profile and select a FortiClient installer. See [Endpoint profiles on page 15](#).
5. Apply a profile to a workgroup or domain, an endpoint group, or an organizational group:
  - a. Right-click on the organizational unit, group, domain, or workgroup in the *Endpoint* pane.
  - b. From the right-click menu, select *Assign profile*, then select the name of the profile that is to be assigned to that unit.

Depending on the configuration of the selected profile, FortiClient will be installed on the endpoints to which the profile is applied.

After FortiClient installation, the endpoint user must connect FortiClient Telemetry to FortiGate or FortiClient EMS to receive the profile configuration and complete the endpoint management setup. See [Connect FortiClient Telemetry to FortiClient EMS on page 18](#).

6. For endpoints that are managed by the EMS, select a domain or group to view and customize the applied profile, view a list of the endpoints in that group, and run quick and full virus scans on the endpoints.  
For endpoints that are managed by a FortiGate device, no scanning is done via the EMS.

## Discover endpoints

You can use the following methods to discover endpoints:

- Use an Active Directory (AD) server to discover endpoints
- Scan local workgroups to discover endpoints

You can add AD servers under the *Domains* heading. Workgroup computers are listed under *Other groups* in the *Endpoints* pane.

Computers using Microsoft Windows' Computer Browser Service can be discovered and added to EMS.

## Use AD servers to discover endpoints

### To use AD servers:

1. From the *Endpoint* pane toolbar, click *Add a new domain*. The *Domain Settings* pane opens.
2. Enter the following information.

<b>Group Name</b>	Enter a name for the group.
<b>Server IP/Name</b>	Enter the AD server IP address or name.
<b>Server Port</b>	Select the server port.
<b>Distinguished Name</b>	<p>Enter the distinguished name (optional).</p> <p>Format:</p> <p style="padding-left: 40px;">OU=&lt;organizational_unit&gt;, ..., OU=&lt;organizational_unit&gt;, DC=&lt;domain_name&gt;, DC=&lt;domain_postfix&gt;</p> <p>Example:</p> <p style="padding-left: 40px;">OU=Americas, OU=Spectrum, DC=Spectrum, DC=ca</p>
<b>Bind Type</b>	Select the bind type. If <i>Regular</i> is selected, enter the <i>User DN</i> and <i>Password</i> . Select whether to show the password and use the secure LDAPS connection protocol.

3. Select *Test* to test the domain settings.
4. If the test is successful, select *Save* to save the new domain.  
If the test is not successful, correct the information as required, and then test the settings again.

## Scan local workgroups to discover endpoints

### To scan local workgroups:

1. Select *View > Settings*.
2. Enable the *Scan local workgroups* option.
3. Select *Save*.

## FortiClient Telemetry Gateway IP Lists

The FortiClient Telemetry Gateway IP List identifies IP addresses for FortiGate and/or EMS to which endpoints can connect FortiClient Telemetry. You can create one or more FortiClient Telemetry Gateway IP Lists, and assign the list to a domain or workgroup.

### Create FortiClient Telemetry Gateway IP Lists

**To create a FortiClient Telemetry Gateway IP List:**

1. Go to *FortiClient Telemetry Gateway IP List*.
2. Click the + button.
3. Configure the options, and select *Save*.

### Assign FortiClient Telemetry Gateway IP Lists

**To assign FortiClient Telemetry Gateway IP Lists:**

1. Right-click a domain or workgroup, select *Assign FortiClient Telemetry Gateway IP List*, and select a FortiClient Telemetry Gateway IP List.

## FortiClient installers

FortiClient EMS automatically connects to FortiGuard Distribution Network (FDN) to provide access to FortiClient installers that you can use with FortiClient EMS profiles. You can customize the FortiClient installers by using FortiClient EMS. If a connection to FDN is not available, you must manually download FortiClient installers to use with FortiClient EMS.

Alternately you can create custom FortiClient installers by using the FortiClient Configurator tool, and then upload the custom installers to FortiClient EMS.

The following services must be enabled and configured on each Windows endpoint before FortiClient is deployed to them:

- Task Scheduler: Automatic
- Windows Installer: Manual
- Remote Registry: Automatic



The Windows Firewall must be configured to allow the following inbound connections:

- File and Printer Sharing (SMB-In)
  - Remote Scheduled Tasks Management (RPC)
- 

For AD group deployments, an AD administrator account is required. For non-AD deployments, the installer URL can be shared with users, who can then download and install FortiClient manually.

**To add an installer:**

1. Select **View > Software Manager**. The *FortiClient Software Manager* pane opens.
2. Select **Add** to open the *Add Installer* window.

3. Configure the following settings:

<b>Name</b>	Enter a name for the installer.
<b>Notes</b>	Optionally, enter notes describing the installer.
<b>OS</b>	Select the OS to which the installer will apply, <i>Windows</i> or <i>Mac OS X</i> .
<b>FortiClient Version</b>	Select the FortiClient version that the installer will install, or select <i>Upload</i> to upload an installer file.
<b>Patch Version</b>	Select the patch version of FortiClient that will be installed. Select <i>Keep software updated to latest patch release</i> to force the software to automatically update to the latest patch.
<b>Keep software updated to latest patch release</b>	Select to keep FortiClient updated to the latest available patch release.
<b>Features to Install</b>	Select the features to install, one of: <ul style="list-style-type: none"> <li>• <i>All features</i></li> <li>• <i>Security only</i></li> <li>• <i>VPN only</i></li> <li>• <i>AntiVirus, Web Filtering, and Vulnerability Scan only</i></li> <li>• <i>Web Filtering only</i></li> <li>• <i>Vulnerability Scan only</i></li> <li>• <i>Application Firewall only</i></li> <li>• <i>Application Firewall, Web Filtering, and Vulnerability Scan</i></li> <li>• <i>Application Firewall, VPN, Web Filtering, and Vulnerability Scan</i></li> </ul>

<b>This FortiClient will be managed by</b>	Select whether <i>EMS</i> or <i>FortiGate</i> will manage the endpoint.
<b>Automatic Registration</b>	Turn automatic registration on or off. When enabled, after installation FortiClient will automatically register to the first possible IP in the registration IP list.
<b>Desktop Shortcut</b>	Select whether or not a desktop shortcut will be created for FortiClient on the endpoint.
<b>Start menu shortcut</b>	Select whether or not a start menu shortcut will be created for FortiClient on the endpoint.

4. Select *Save* to create the new installer.

## Endpoint profiles

You can assign endpoint profiles to device groups or domains. If you do not apply an endpoint profile to a specific group or domain, the default endpoint profile is automatically applied.

You can create endpoint profiles by using EMS, or you can import FortiClient profiles from FortiGate to EMS.

## Create endpoint profiles

### To create endpoint profiles:

1. From the *Endpoint Profiles* pane toolbar, click *Add a new profile*. The *Endpoint Profile* pane opens. Alternately, you can click the *Clone* icon in the default profile row to create a new endpoint profile based on the default endpoint profile.
2. Optionally, click *Advanced* to configure the endpoint profile by directly editing the XML code.
3. If using the basic configuration option, configure the following settings:

<b>Profile Name</b>	Enter a name for the endpoint profile, from 1 to 128 character with no special characters.
<b>Install Options</b>	Select a FortiClient installer to include in the endpoint profile. See <a href="#">FortiClient installers on page 13</a>
<b>Feature Settings</b>	Configure endpoint profile feature settings.

<b>AntiVirus Protection</b>	<p>Enable antivirus protection. Configure the following options:</p> <ul style="list-style-type: none"> <li>• <i>Real-time Protection</i>: Enable real-time protection and configure options.</li> <li>• <i>Scheduled Scan</i>: Enable scheduled scans, then configure the schedule and scan type.</li> <li>• <i>Exclusions</i>: Enable exclusions from the scan. Enter fully qualified file and folder paths in the text boxes to exclude them from antivirus protection.</li> </ul>
<b>Web Filtering</b>	<p>Enable web filtering.</p> <ul style="list-style-type: none"> <li>• <i>Client Web Filtering when On-Net</i>: Enable client web filtering when On-Net.</li> <li>• <i>Enable FortiGuard URL categorization</i>: Block, Warn, Allow, or Monitor specific categories of web sites. See the <a href="#">FortiGuard</a> web site for a list of the available categories and subcategories.</li> <li>• <i>Rate ip addresses</i>: Select to rate IP addresses.</li> <li>• <i>Exclusion List</i>: Enter specific URLs to block or allow. Wildcard characters and Perl Compatible Regular Expressions (PCRE) can be used.</li> </ul>
<b>Application Firewall</b>	Enable application control. See the <i>FortiClient EMS Administration Guide</i> for more information.
<b>VPN</b>	Enable VPN use. See the <i>FortiClient EMS Administration Guide</i> for more information.
<b>Vulnerability Scan</b>	Enable vulnerability scan. See the <i>FortiClient EMS Administration Guide</i> for more information.
<b>System Settings</b>	Configure profile system settings.
<b>UI Options</b>	Enable <i>Dashboard Banner</i> to display the dashboard banner in the FortiClient console on endpoints.
	Enable <i>Password Lock Configuration</i> . Enter a password in the <i>Password</i> field. Select <i>Show Password</i> to show the password in plain text.
<b>Log Settings</b>	Select <i>Client-based logging when On-Net</i> to enable logging when FortiGate is being used as a DHCP server.
	<p>Select <i>Upload Logs to FortiAnalyzer/FortiManager</i> to upload logs to the FortiAnalyzer or FortiManager device at the specified address or hostname.</p> <p>Select the log upload schedule, either hourly or daily.</p>
<b>Update Settings</b>	<p>Select <i>Use FortiManger for client software/signature update</i> to configure FortiClient to obtain antivirus signatures and software updates from the FortiManager device at the specified IP address or hostname.</p> <p>If required, enable <i>Failover to FDN when FortiManager is not available</i>.</p>



<b>Endpoint Control Settings</b>	Select <i>Silent Registration</i> to enable endpoints to connect FortiClient Telemetry with FortiGate/EMS without user interaction.
	Select <i>Log off when user logs out of Windows</i> to allow FortiClient to log off the network when the endpoint user logs out of Windows.
	Select <i>Disable Unregister</i> to prevent managed endpoints from disconnecting FortiClient Telemetry from FortiGate/EMS.
<b>Other Options</b>	Select <i>Onnet Subnets</i> to identify the IP addresses/masks of the subnets.
	Select <i>Install CA Certificate on Client</i> to select a certificate to install on FortiClient endpoints. You must add certificates to FortiClient EMS before you can select them in profiles. Go to <i>View &gt; CA Certificate Management</i> .
	Select <i>FortiClient Single Sign-On mobility agent</i> to enable the single sign-on mobility agent. Enter the IP address or hostname, port, and pre-shared key. Select <i>Show Password</i> to show the password.
<b>iOS</b>	Select <i>Distribute Configuration Profile (.mobileconfig file)</i> to select a .mobileconfig file to distribute with FortiClient.

4. Select *Save* to save the endpoint profile.
5. After creating the endpoint profile, you can apply the endpoint profile to AD organizational units, groups, or workgroups with the right-click menu.

## Import FortiClient profiles from FortiGate

In FortiOS, endpoint profiles are called FortiClient profiles. You can import a FortiClient profile into EMS.

### To import a FortiClient profile from FortiGate:



This feature requires a FortiGate running FortiOS 5.4.0 and later.

1. From the *Endpoint Profiles* pane toolbar, click *Import profile from FortiGate*. The *Import Profile from FortiGate* window opens.

2. Configure the following settings:

<b>Server IP / Hostname</b>	Enter the IP address and hostname of the FortiGate device from which the profile is being imported, in the format: <ip address>.
<b>VDOM</b>	Enter a VDOM name from the FortiGate if applicable.
<b>Username</b>	Enter the device's login username.
<b>Password</b>	Enter the device's login password.

3. Select *Next*.
4. If a registration key has been configured, enter it in the *Registration Key* field, then select *Next*.
5. Select the FortiClient profiles from the FortiGate that will be imported to the EMS.  
The selected FortiClient profiles are automatically named and listed in the *Profile to Import* box. Selecting a FortiClient profile from the *Profile to Import* box will display a preview of the FortiClient profile, in XML, in the *Profile Preview* box.
6. Optionally, select whether to automatically synchronize the profile in EMS when you update the profile in FortiOS by enabling the *Auto-sync every* option and specifying a time interval.
7. Select *Import* to import the selected FortiClient profiles.  
The imported FortiClient profiles will be listed under the *Endpoint Profiles* pane in a group named after the FortiGate device from which they were imported.



Imported FortiClient profiles are read-only in FortiClient EMS. However, you can enable automatic synchronization of imported profiles in the profile settings. Then when you update the profile in FortiGate, the changes are automatically updated in FortiClient EMS.

8. To add an installer to the profile, select a profile to open the *Endpoint Profiles* page, then select an installer in the *Install Options* tab.  
Custom installers can also be created. See [FortiClient installers on page 13](#).

## Connect FortiClient Telemetry to FortiClient EMS

Endpoint users must connect FortiClient Telemetry to FortiGate or FortiClient EMS. After FortiClient Telemetry is connected, a profile is downloaded to FortiClient, and the endpoint device is managed.

This section describes how to manually connect FortiClient Telemetry. You can configure automatic FortiClient Telemetry connection by creating a FortiClient Telemetry Gateway IP List in FortiClient EMS, and assigning the list to one or more gateways or workgroups. Alternately, you can create a custom FortiClient installer that includes a FortiClient Telemetry Gateway IP List. For more information, see the *FortiClient EMS Administration Guide*.

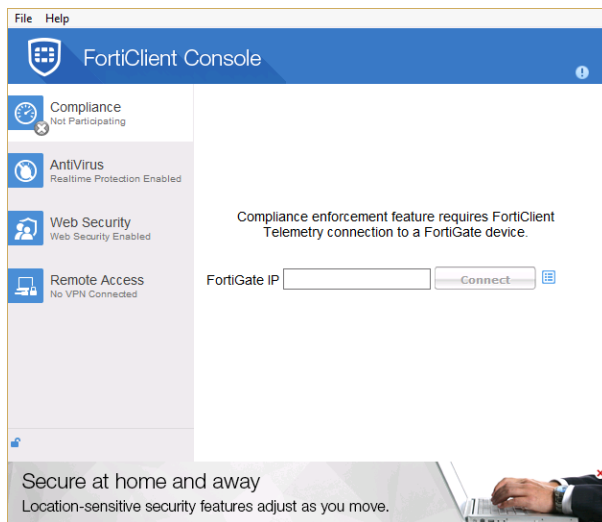


The registration terminology changed in FortiClient 5.4.1 and later. FortiClient 5.4.1 and later connects FortiClient Telemetry to FortiGate/EMS to be managed. FortiClient 5.4.0 and earlier, registers to FortiGate/EMS to be managed.

For more information about FortiClient Telemetry connections, see the *FortiClient Administration Guide*, available in the [Fortinet Document Library](#).

**To manually connect FortiClient Telemetry:**

1. Ensure FortiClient 5.4.1 or later is installed on the endpoint device.
2. In FortiClient console, click the *Compliance* tab.



3. In the *FortiGate IP* box, type the IP address configured in FortiClient EMS, and click *Connect*.  
For information about the IP address configured in FortiClient EMS, see [Start FortiClient EMS on page 9](#).  
FortiClient Telemetry connects to FortiClient EMS.



**FORTINET®**

High Performance Network Security



Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.